

2000-03-21

AWAPATENT ABKontor/Handläggare
Malmö/Gunilla Larsson**ICONIZER AB**

Ansökningsnr

Huvudfaxen Kassar

Vår referens
SE-2000876

1

VERIFIKATIONSSYSTEMTekniskt område

Föreliggande uppfinning avser ett system för analys av en användares signatur, varvid systemet innefattar en användarenhet och en kontrollanordning, varvid användarenheten är anordnad att registrera en signatur, som användaren skriver med användarenheten, och att skicka signaturen till kontrollanordningen, som är anordnad att mottaga signaturen. Uppfinningen avser vidare en kontrollanordning för analys av en användares signatur, som är inskriven med en användarenhet, varvid kontrollanordningen är anordnad att mottaga signaturen, samt ett sätt att analysera en signatur.

Bakgrundsteknik

Namn-teckningen har länge använts för att öka säkerheten vid användning av olika typer av betalningssystem. Exempelvis används namnteckningen på checkar, vid kortbetalningar och girobetalningar som en extra försäkring om att en betalare verkligen är den som han utger sig för att vara. Namnteckningen kan skrivas med en vanlig penna eller med en elektronisk penna. Med elektroniska pennor finns möjligheten att utöka antalet parametrar som beskriver namnteckningen. Förutom att man kan beräkna samma parametrar som på en vanligt inskriven namnteckning, som t ex bokstävernas absoluta storlek och lutning, kan man också exempelvis beräkna hur hårt den elektroniska pennan trycks mot underlaget och hastigheten med vilken namnteckningen skrivs med. Detta kan man läsa i artikeln "Optimisation issues in dynamic and static signatures verification" i Handwriting Analysing and Registration. (ref. No. 1998/440), IEE Third European Workshop, 1998, page 5/1-5/6, skriven av C.C. Allgrove and M.C. Fairhurst, som också beskriver ett sätt på vilket en verifikationsdatabas kan byggas upp. I artikeln beskrivs



#9

PATENT
3782-0109P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant: Sven-Olof KARLSSON Conf.: 1159
Appl. No.: 09/812,899 Group: 2183
Filed: March 21, 2001 Examiner:
For: SECURE SIGNATURE CHECKING SYSTEM

RECEIVED
AUG 08 2001
Technology Center 2100L E T T E RAssistant Commissioner for Patents
Washington, DC 20231

August 6, 2001

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
SWEDEN	0000943-1	March 21, 2000

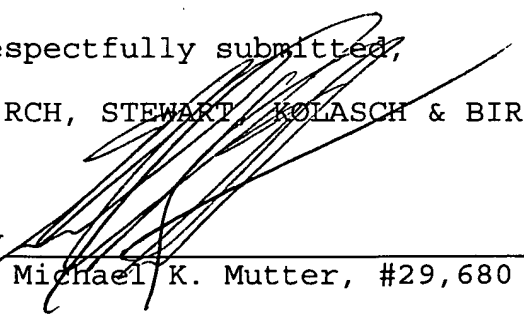
A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By


Michael K. Mutter, #29,680MKM/abs
3782-0109PP.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

Attachment

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen



RECEIVED
AUG 0 8 2001
Technology Center 2100

Intyg Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

- (71) Sökande Anoto AB, Lund SE
Applicant (s)
- (21) Patentansökningsnummer 0000943-1
Patent application number
- (86) Ingivningsdatum 2000-03-21
Date of filing

Stockholm, 2001-03-15

För Patent- och registreringsverket
For the Patent- and Registration Office


Hjordis Segerlund

Avgift
Fee 170:--

**PATENT- OCH
REGISTRERINGSVERKET
SWEDEN**

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

2000 -03- 2 1

Huvudfaxen Kassan

2

ett verifikationssystem som innefattar en verifikations-
databas i vilken referensmodeller för ett antal namn-
teckning lagras. En persons namnteckning varierar något
5 varje gång den skrivs och referensmodellen tar hänsyn
till dessa variationer. Då en referensmodell byggs upp
skriver användaren in sin signatur ett antal gånger och
man får ett intervall inom vilket användarens signatur
ligger. För att förbättra referensmodellen kan den eller
de signaturer, som skiljer sig mycket från användarens
10 andra inskrivna signaturer, filtreras bort.

Sammanfattning av uppfinningen

Ett ändamål med uppfinningen är att åstadkomma ett
system som ökar säkerheten vid användning av elektroniska
signaturer.

15 Detta ändamål uppnås med ett system för analys av en
användares signatur enligt krav 1, en kontrollanordning
enligt krav 13 och ett sätt enligt krav 19.

Närmare bestämt avser uppfinningen enligt en första
aspekt ett system för analys av en användares signatur,
20 varvid systemet innefattar en användarenhet och en kon-
trollanordning, varvid användarenheten är anordnad att
registrera en signatur när användaren skriver med använ-
darenheten, och att skicka signaturen till kontrollanord-
ningen, som är anordnad att mottaga signaturen, varvid
25 kontrollanordningen vidare är anordnad att bygga en sig-
naturmodell baserad på signaturen, att göra en kontroll
av signaturmodellens unikheter och att efter kontrollen av-
ge en signal, som indikerar signaturmodellens unikheter,
till användarenheten.

30 Uppfinningen bygger på idén att ge en användare en
möjlighet att kontrollera hur unik hans eller hennes
signatur är. Med en unik signatur menas inte enbart att
signaturen är olik andra signaturer, utan också exempel-
vis att den innehåller särdrag som medför en bättre
35 maskinigenkänning av signaturen. Signaturen är vanligtvis
användarens namnteckning, men kan också vara en symbol
eller någon typ av tecken. Fördelen med att användaren

2000-03-21

Huvudfaxen Kassan

3

kan kontrollera unikheten i hans eller hennes signatur är alltså att användaren kan få en indikation på hur bra signaturen är, dvs exempelvis hur svår den är att förfälska, förväxla med en annan signatur eller hur enkel den är att behandla i ett maskinigenkänningsprogram.

Användarenheten eller del av användarenheten kan vara utformad som en penna med vilken användaren skriver sin signatur och kan exempelvis vara en digital penna. Användarenheten registrerar signaturen och skickar en representation av signaturen vidare till kontrollanordningen.

Signaturen mottages av kontrollanordningen. När signaturen mottagits kan en eller flera parametrar bestämmas. Dessa parametrar kan exempelvis vara signaturens längd, bokstävernans lutning och/eller antalet böjar i signaturen. En böj kan definieras som en större förändring i riktning hos signaturen. Parametrarna kan sedan jämföras med förutbestämda miniminivåer inom vilka de ska ligga för att signaturen ska betraktas uppfylla vissa unikhetskrav. I ett mycket enkelt fall utgörs signaturmodellen av en signatur och ovan nämnda kontroll kan vara själva unikhetskontrollen. I ett mycket enkelt exempel på en unikhetskontroll sker kontroll på endast en parameter t ex antalet böjar i signaturen. Om signaturen i detta fall bara utgörs av ett streck, vilket innebär att antalet böjar är noll, och antalet böjar är bestämt till att var större eller lika med 10 för att signaturen ska bedömas vara unik, så bedömer kontrollanordningen att signaturen inte är unik. Förutom att jämföra parametern med en förutbestämd gränsnivå kan den också jämföras med en eller flera tidigare lagrade signaturers parametrar. Om vi tar det föregående fallet, där parametern är antal böjar, kan det ha bestämts att för att en signatur ska betraktas som unik måste den skilja sig två steg i antalet böjar från tidigare lagrade signaturer.

Företrädesvis utförs jämförelsen dels med den förutbestämda gränsnivån och dels med tidigare lagrade sig-

2000-03-21

Huvudfaxen Kassan

4

naturer. Detta är givetvis en förenklad förklaring av kontrollen av signatursens unikhets. Företrädesvis används en mängd olika parametrar för att göra kontrollen av signatursens unikhets. Signaturmodellen kan byggas upp av ett antal mottagna signaturer från samma användare, men kan också utgöras av bara den mottagna signaturen, som var det enkla fallet som nämndes här ovan. Om signaturmodellen byggs upp av ett antal signaturer kan ovan nämnda minimikravskontroll utföras för varje signatur som sedan bygger upp signaturmodellen. Om minimikravskontrollen utförs byggs signaturmodellen upp av signaturer som åtminstone uppfyller vissa kriterier. Kontrollanordningen utför sedan en kontroll på hur unik signaturmodellen är. För att utföra kontrollen och värdera de olika parametrarna kan olika klassificeringsmetoder användas. Vanligtvis används vid dessa metoder en klassifikator, som exempelvis kan vara ett neuralt nätverk. En klassifikator kan "tränas" genom att man matar in en signaturs parametrar och jämför svarsvärdet som kommer ut med det resultat man vill ha ut. Om svarsvärdet inte är det man önskade, ändrar man lite på klassifikatorn och matar åter in parametrarna och jämför svarsvärdet med det önskade. Man fortsätter med detta tills man får ett önskat resultat. När en unikhetskontroll ska göras på en signatur, vilken signatur inte behöver finnas lagrad i det neurala nätverket, kan dess parametrar matas in i klassifikatorn. Svarsvärdet ut från klassifikatorn kan vara ett unikhetsmått.

Klassifikatorn kan också ge en indikation på hur nära en inmatad signaturmodell ligger en tidigare lagrad signaturmodell.

Om signaturmodellen innefattar mer än en signatur sker klassificering vanligtvis efter varje mottagen signatur och på så sätt kan signaturmodellen byggas upp.

När kontrollen av signaturmodellens unikhets är klar skickar kontrollanordningen en signal till användarenheten för att informera användaren om hur unik hans signa-

2000-03-21

Huvudfaxen Kassar

5

tur är. Om unikheten inte är tillräcklig kan kontrollanordningen skicka med information om vad som kan ändras i signaturen för att få den unik. Signalen kan också enbart vara en klarsignal, som meddelar att signaturen är unik
5 eller en signal som enbart meddelar att signaturen inte är tillräckligt unik.

I en annan utföringsform av systemet är signaturmodellen signaturen.

Ibland kan det vara önskvärt med en snabb kontroll
10 av signaturens unikhets och användaren skriver då endast in sin signatur en gång. Signaturmodellen är då denna signatur och kontrollanordningen är då anordnad att kontrollera unikheten hos denna enda signatur.

I en utföringsform av systemet är kontrollanordningen anordnad att bygga upp signaturmodellen av ett
15 antal från samma användare mottagna signaturer.

Signaturmodellen byggs med fördel upp av ett antal från samma användare inskrivna signaturer. Fördelen med signaturmodellen är att den tar hänsyn till variationer i
20 samma användares signatur. En användare har ofta små variationer mellan olika inskrivningar av signaturen. Signaturmodellen kan förbättras ytterligare genom att exempelvis plocka bort den signatur som skiljer sig mest från de övriga.

25 I en annan utföringsform av systemet är kontrollanordningen anordnad att i kontrollen av signaturmodellens unikhets beräkna minst en för signaturmodellen kännetecknande parameter och att göra en kontroll av nämnda minst en parameter.

30 Det finns många parametrar som kan vara intressanta att undersöka i signaturmodellen för att kontrollera dess unikhets. En parameter, som nämndes ovan, kan räcka för att göra en unikhetskontroll, men företrädesvis används ett flertal parametrar, eftersom signaturens unikhetskontroll blir säkrare. Med tillgång till ett stort antal
35 parametrar kan man få en bättre klassificering. Unikhetskontrollen behöver inte göras direkt på parametern, utan

2000-03-21

Huvudfaxen Kassar

6

parametern kan matas direkt till en klassifikator. Klassifikatorn ger ett svarsvärde som ger ett unikhetsmått och som unikhetskontrollen kan göras på.

En parameter som kan användas för unikhetskontrollen
5 är exempelvis signaturens utbredning. Utbredningen kan exempelvis beräknas som ett höjd-längd-förhållande eller som en absolut längd. Andra parametrar kan t ex vara antalet böjar, derivatan av rörelsen i x-led, y-led och riktning, signaturens absoluta storlek, korsningar, kurvor,
10 linjeslut och trycket med vilken signaturen skrivs in. Ytterligare parametrar kan vara lutning på bokstäver och ord.

I en utföringsform av systemet enligt uppfinningen är kontrollanordningen anordnad att för kontrollen av
15 nämnda minst en parameter kontrollera att nämnda minst en parameter ligger över en förutbestämd unikhetsgränsnivå.

Unikhetsgränsnivån sätts till en nivå som om signaturmodellens nämnda minst en parameter understiger denna nivå bedöms signaturmodellen inte vara unik. Om den där-
20 emot överstiger eller ligger på denna nivå betraktas signaturen som unik. Givetvis kan denna nivå definieras på så sätt att om nivån understiger den förutbestämda unikhetsgränsnivån bestäms signaturen vara unik. Hur kontrollanordningen behandlar nämnda minst en parameters
25 jämförelse med unikhetsgränsnivån kan definieras i systemet. En fördel med att använda denna unikhetsgränsnivå är att man beroende på hur mycket signaturmodellen skiljer sig från unikhetsgränsnivån kan få en indikation på hur unik användarens signatur är.

30 Signalen från kontrollanordningen till användarenheten kan innefatta information om signaturmodellen ligger över, under eller på gränsen till unikhetsgränsnivån. Signalen kan också innefatta information om hur mycket den avviker från unikhetsgränsnivån. Fördelen med
35 detta är att användaren får information om hur säker hans eller hennes signatur är och beroende på detta får användaren exempelvis en indikation till vad signaturen kan

2000 -03- 2 1

Huvudfaxen Kassar

7

användas. Om signaturen har en hög grad av unikheter kan användaren exempelvis använda den i ett betalningssystem.

Kontrollanordningens unikhetsgränsnivå kan justeras beroende på inom vilket användningsområde användarens signatur är tänkt att användas. Systemet kan vara så anordnat att användarenheten skickar information om användningsområdet tillsammans med signaturen till kontrollanordningen. Kontrollanordningen använder då den till detta användningsområde hörande unikhetsgränsnivån. Om en klassifikator används kan unikhetsgränsnivån vara en svarsgränsnivå. Om svarsgränsnivån från klassifikatorn höjs, så kan säkerhetsnivån höjas. Värdet ut från klassifikatorn kan jämföras med svarsgränsnivån för att bedöma om signaturen är unik.

I en annan utföringsform av systemet enligt uppfinningen innefattar nämnda signal information om vad användaren ska ändra på i sin signatur för att nämnda minst en parameter ska hamna över unikhetsgränsnivån.

Fördelen med att användaren får information om vad som ska ändras i signaturen för att den ska bli unik är att användaren på ett snabbt och enkelt sätt kan få fram en unik signatur. Användaren behöver inte slumpvis ändra olika delar av signaturen tills den blir bedömd unik, utan kan få direkt information om vad som kan ändras.

I en utföringsform av systemet är kontrollanordningen vidare anordnad att klassificera signaturen.

Med fördel klassificerar kontrollanordningen varje mottagen signatur. Om signaturmodellen ska innefatta mer än en signatur klassificeras varje signatur för att bygga upp signaturmodellen.

För att underlätta klassificeringen av signaturen används företrädesvis ett antal parametrar. Fördelen med klassificering är att det går snabbare att kontrollera signaturens unikheter. Som nämnts ovan finns det olika metoder för att utföra en klassificering.

I ytterligare en utföringsform av systemet är kontrollanordningen anordnad att, i kontrollen av signatur-

2000 -03- 2 1

Huvudfoxen Kassa

8

modellens unikheter, jämföra denna med tidigare lagrade signaturmodeller.

5 För att signaturen också ska vara unik i förhållande till tidigare lagrade signaturer jämförs signaturmodellen med tidigare lagrade signaturmodeller, för att de lagrade signaturmodellerna inte ska vara för lika varandra. Signalen från kontrollanordningen till användarenheten kan ge information till användaren om vad användaren bör ändra i sin signatur för att den inte ska vara för lik en tidigare av en annan person inskriven signatur. Hur mycket två inskrivna signaturer bör skilja sig åt kan bero på signatursens användningsområde. Denna jämförelse utförs med fördel i kombination med kontrollen av att signaturmodellen ligger över en förutbestämd unikhetsgränsnivå.

10 I en utföringsform av systemet registreras signaturen som en sekvens av koordinater som beskriver användarenhetens förflyttning när användaren skriver sin signatur med användarenheten.

20 Genom att beskriva signaturen som en sekvens av koordinater kan man på ett enkelt sätt beräkna olika parametrar ur signaturen.

I en annan utföringsform innefattar systemet ett underlag, vilket är försett med ett positionskodningsmönster, som möjliggör beräkning av koordinaterna och från vilket användarenheten är anordnad att registrera sekvensen av koordinater.

30 Användarenheten registrerar mönstret och beräknar lämpligen dess motsvarande koordinatpar. Koordinatparen kan lagras i ett minne i användarenheten. Användarenheten kan vidare vara anordnad att analysera lagrade koordinatpar och omvandla dessa till ett polygontåg som utgör en beskrivning av hur pennan har förflyttats över en yta som är försedd med positionskodningsmönstret, vilken förflyttning är användarens signatur. Polygontåget kan sedan överföras till kontrollanordningen för unikhetskontroll. Tidpunkten då olika koordinatpar registreras kan också registreras för att få ytterligare en parameter.

2000 -03- 2 1

Huvudfoxen Kassan

9

I en utföringsform av systemet innefattar användarenheten en optisk sensor och bildbehandlingsorgan för registrering av signaturen.

Den optiska sensorn upptar bilder och bildbehandlingsorgan behandlar bilderna, vilket innefattar att bestämma koordinaterna utifrån innehållet i bilderna, varvid innehållet kan vara ovannämnda positionskodningsmönster.

I en utföringsform av systemet är kontrollanordningen anordnad i en verifikationsdatabas.

Med fördel är kontrollanordningen anordnad i en verifikationsdatabas i vilken det kan finnas lagrat ett flertal olika signaturer i form av signaturmodeller. Om signaturmodellen sedan tidigare finns lagrad i minnet kan verifikationsdatabasen också bestyrka signaturens riktighet. Detta kan exempelvis ske genom att användarenheten skickar med en användaridentitet till verifikationsdatabasen. Verifikationsdatabasen vet då med vilken signatur en jämförelse ska ske. Den signal som avges till användarenheten kan då informera användaren om hur lik signaturen är den lagrade. Kanske har användarens signatur förändrats.

Uppfinningen avser också enligt en andra aspekt en kontrollanordning för analys av en användares signatur, som är inskriven med en användarenhet, varvid kontrollanordningen är anordnad att mottaga signaturen, varvid kontrollanordningen vidare är anordnad att bygga en signaturmodell baserad på signaturen, att göra en kontroll av signaturmodellens unikheter och att avge en signal, som indikerar signaturmodellens unikheter, till användarenheten.

Enligt en tredje aspekt avser uppfinningen ett sätt att analysera en signatur innefattande stegen att med en användarenhet registrera en signatur, att skicka vidare en representation av signaturen till en kontrollanordning, att i kontrollanordningen bygga upp en signaturmodell, att i kontrollanordningen göra en kontroll av

2000 -03- 2 1

Huvudfaxen Kassan

10

signaturmodellens unikheter och att efter kontrollen avge en signal, som indikerar signaturmodellens unikheter, till användarenheten.

- 5 Fördelarna med kontrollanordningen och sättet framgår av diskussionen ovan. De särdrag som diskuterats angående systemet gäller också i tillämpliga delar för kontrollanordningen och sättet.

Kort beskrivning av ritningarna

- 10 Uppfinningen kommer att beskrivas närmare i det följande under hänvisning till bifogade ritningar.

Fig 1 är en schematisk bild över en utföringsform av systemet.

Fig 2 visar ett exempel på en användarenhet.

Fig 3 visar ett exempel på en handskriven signatur.

15 Beskrivning av en föredragen utföringsform

- I fig 1 visas en utföringsform av systemet enligt uppfinningen. Systemet innefattar ett antal användarenheter 1 och en kontrollanordning integrerad med en verifikationsdatabas 2. För enkelhetens skull visas i fig 1
20 bara en användarenhet. Verifikationsdatabasen 2 och användarenheten 1 kommunicerar via ett datornätverk 3. Användarenheten 1 är utrustad med en nätverksanslutningsenhet 4 som i detta exempel kan kommunicera trådlöst med verifikationsdatabasen 2. Nätverksanslutningsenheten är i
25 detta fall integrerad med användarenheten, men kan alternativt vara en mobiltelefon, en dator eller någon annan lämplig enhet som har ett gränssnitt mot ett nätverk, exempelvis Internet eller ett lokalt företagsnät.

Skrivunderlag

- 30 I fig 1 visas ett exempel på ett skrivunderlag 5 som till storlek och material liknar ett vanligt magnetkort. Skrivunderlaget 5 har ett skrivområde 6 som kan förses med koordinater, som kan avläsas av den digitala pennan 1. Koordinaterna kan vara angivna i explicit eller kodad
35 form. I detta exempel är skrivunderlaget 5 försett med ett positionskodningsmönster 7. Mönstret 7 visas schema-

2000-03-21

Huvudfaxen Kassar

11

tiskt som ett antal prickar på en del av skrivunderlaget 5.

Skrivområdet 6 är avsett för handskriven information, vilket i detta fall är användarens namnteckning.

- 5 Skrivunderlaget 5 kan vara utformat av sådant material så att signaturen kan suddas ut efter att ha skrivits. Alternativt kan kombinationen av penna och skrivunderlag vara sådan att inget färgämne avsätts på skrivunderlaget när användaren skriver signaturen.

- 10 Positionskodningsmönstret 7 kan vara av sådan typ som visas i US 5,852,434, där varje position kodas av en specifik symbol.

- Positionskodningsmönstret 7 är dock med fördel av den typ som visas i sökandens ovannämnda ansökningar
- 15 SE 9901954-9 och SE 9903541-2, där varje position kodas av ett flertal symboler och varje symbol bidrar till kodningen av flera positioner. Positionskodningsmönstret 7 byggs upp av ett fåtal typer av symboler. Ett exempel visas i SE 9901954-9 där en större prick representerar en
- 20 "etta" och en mindre prick representerar en "nolla". Ett annat exempel visas i SE 9901954-9, där fyra olika förskjutningar av en prick i förhållande till en rasterpunkt kodar fyra olika värden.

Användarenheten

- 25 I fig 2 visas ett exempel på en användarenhet, som i detta fall utgörs av en digital penna 1. Den innefattar ett hölje 11, som är format ungefär som en penna. I höljets kortända finns en öppning 12. Kortänden är avsedd att ligga an mot eller hållas på litet avstånd från den
- 30 yta på vilken positionsbestämningen skall ske.

Höljet inrymmer i huvudsak en optikdel, en elektronikdel och en strömförsörjning.

- Optikdelen innefattar minst en lysdiod 13 för belysning av den yta som skall avbildas och en ljuskänslig
- 35 areasensor 14, exempelvis en CCD- eller CMOS-sensor, för registrering av en tvådimensionell bild. Eventuellt kan pennan dessutom innehålla ett linssystem.

Ink i Patent- och reg.verket

2000-03-21

12

Huvudfaxen Kassan

Strömförsörjningen till användarenheten erhålls från ett batteri 15 som är monterat i ett separat fack i höljet.

Elektronikdelen innehåller en processor 16 som är programmerad till att läsa in en bild från sensorn 14, identifiera symboler i bilden, bestämma vilka två koordinater som symbolerna kodar och att lagra dessa koordinater i sitt minne. Processorn 16 är vidare programmerad till att analysera lagrade koordinatpar och omvandla dessa till ett polygontåg som utgör en beskrivning av hur pennan har förflyttats över en yta som är försedd med positionskodningsmönstret, vilken förflyttning exempelvis kan vara användarens signatur. Slutligen är processorn programmerad till att generera ett meddelande som innehåller polygontåget och att skicka denna information till verifikationsdatabasen 2 via sändtagaren 19 och nätverksanslutningsenheten 4.

Den digitala pennan 1 innefattar vidare en pennspets 17, med vars hjälp användaren kan skriva vanlig färgämnesbaserad skrift som samtidigt registreras av pennan 1 med hjälp av positionskodningsmönstret. Pennspetsen 17 är in- och utfällbar så att användaren kan styra om den skall användas eller ej.

Den digitala pennan 1 innefattar vidare knappar 18 med vars hjälp enheten aktiveras och styrs. Den har också en sändtagare 19 för trådlös kommunikation, t ex med IR-ljus eller radiovågor, med externa enheter.

Kontroll av en signaturs unikhet

I fig 1 visas en utföringsform av uppfinningen i vilken användarenheten är en digital penna 1 och kontrollanordningen är anordnad i en verifikationsdatabas 2. Verifikationsdatabasen 2 kan betjäna ett flertal digitala pennor 1. Den digitala pennan 1 är anordnad att överföra information som genereras av användaren till verifikationsdatabasen 2. I detta fall överförs informationen via en nätverksanslutningsenhet 4 som är integrerad med den digitala pennan 1. Verifikationsdatabasen är realiserad

2000 -03- 2 1

Huvudfaxen Kassan

13

i en dator som är uppbyggd med en eller flera processorer, minne av olika slag, periferienheter och med en ny programvara för att utföra de här beskrivna funktionerna. Den har också information lagrad i ett minne för att

5 kunna hantera dessa funktioner.

I verifikationsdatabasens 2 minne finns lagrat tidigare inskrivna signaturmodeller och olika unikhetsgränsnivåer. En i verifikationsdatabasen mottagen signaturmodell jämförs med unikhetsgränsnivåerna för kontroll av
10 signaturmodellens unikhhet. Unikhetsgränsnivåerna kan exempelvis vara knutna till olika användningsområden, vilka användningsområden ställer olika krav på säkerhet. Möjligheten kan finnas för en användare att på användarenheten välja vilket användningsområde och/eller vilken
15 säkerhetsnivå signaturen ska ligga på. Denna information kan överföras till verifikationsdatabasen tillsammans med signaturen. Verifikationsdatabasen 2 använder då den gränsnivå som associeras med angivet användningsområde.

När en användare vill undersöka om hans eller hennes
20 signatur är unik skriver hon sin signatur med den digitala pennan 1 på ett skrivunderlag 5. Pennan 1 registrerar elektroniskt signaturen som en sekvens av koordinater. Pennan 1 registrerar också den hastighet, som användaren skriver sin signatur med, genom att pennan registrerar de tidpunkter då pennan passerar koordinaterna. Det
25 är möjligt att också utrusta den digitala pennan 1 med en trycksensor som känner av med vilket tryck signaturen skrivs in. Trycket kan bestämmas vid olika tidpunkter. Sekvensen av koordinater och tidpunkterna vid vilken pennan passerar dessa koordinater skickas via nätverksanslutningsenheten 4 och över datornätverket 3 till verifikationsdatabasen 2. Användaren skriver in signaturen ett
30 antal gånger och användarenheten överför denna information. Signaturen bör skrivas in ett antal gånger, eftersom det så gott som alltid förekommer vissa variationer mellan olika inskrivningar av signaturen och för att kompensera för dessa byggs en signaturmodell upp som

2000 -03- 2 1

Huvudfaxen Kassar

14

sätter upp ramar för hur mycket signaturen får variera för att betraktas som tillhörande samma användare. Verifikationsdatabasen mottager och klassificerar varje signatur. När varje signatur mottages kan en minimikrav-

5 kontroll utföras. Exempelvis kan signaturens längd kontrolleras och om den understiger en förutbestämd miniminivå kan en signal skickas till användarenheten som talar om för användaren att signaturen inte kan godtas. Signalen kan också innefatta information om vad som gör att

10 signaturen inte kan godtas. Varje signatur klassificeras utifrån exempelvis signaturens utbredning. Utbredningen kan exempelvis räknas som ett höjd-längd-förhållande eller som en absolut längd. Andra klassificeringsparametrar kan t ex vara antalet böjar, derivatan av rörelsen

15 i x-led, y-led och riktning, signaturens korsningar, kurvor och linjeslut. Ytterligare parametrar kan vara lutning på bokstäver och ord. Verifikationsdatabasens bedömning och värdering av de olika parametrarna kan exempelvis ske med hjälp av statistiska metoder, frekvensanalys, neurala nätverk eller någon annan klassificeringsmetod som t ex Nearest Neighbour. Vanligtvis används vid dessa metoder en klassifikator. En klassifikator kan "tränas" genom att man matar in parametrar och det resultat som kommer ut jämför man med det resultat

20 man ville ha ut. Om resultatet inte är det man önskade ändrar man lite på klassifikatorn och matar åter in parametrarna och jämför resultatet med det önskade. Man fortsätter med detta tills man får ett önskat resultat. Verifikationsdatabasen 2 kontrollerar att signaturmodellen

30 ligger över en användningsberoende unikhetsgränsnivå. Signaturmodellen kan också jämföras med tidigare lagrade signaturmodeller för att inte den inskrivna signaturen inte ska vara för lik en befintlig signatur. Beroende på användningsområdet bör signaturmodellerna skilja sig åt

35 till en förutbestämd grad.

Verifikationsdatabasen 2 skickar efter kontrollen en signal till pennan 1, vilken signal kan innefatta infor-

2000-03-21

Huvudfoxen Kassan

15

mation om att signaturen är tillräckligt unik eller också att den ej är tillräckligt unik. Om signaturen inte är tillräckligt unik kan signalen också innefatta information om vad användaren kan ändra i sin namnteckning. Om
5 signaturen exempelvis bara utgörs av ett streck, vilket innebär att antalet böjar är noll, och gränsnivån för antalet böjar är bestämt till att var större eller lika med 10 för att signaturen ska bedömas vara unik, så bedömer kontrollanordningen att signaturen inte är unik. Signalen
10 till användarenheten kan då meddela användaren om att han eller hon måste öka antalet böjar i signaturen.

Informationen om vilka förändringar som kan vidtas kan presenteras genom att de områden i signaturen som behöver ändras ringas in, se fig 3. Denna information kan
15 kompletteras med ett textmeddelande, som talar om för användaren vilka förändringar som krävs i de inringade områdena.

Även om en speciell utföringsform av uppfinningen har beskrivits ovan är det uppenbart för fackmannen att
20 många alternativ, modifieringar och variationer är möjliga att åstadkomma i ljuset av ovanstående beskrivning.

Ink. t. Patent- och reg.verket

2000-03-21

Huvudfaxen Kassan

16

PATENTKRAV

1. System för analys av en användares signatur,
5 varvid systemet innefattar en användarenhet (1) och en
kontrollanordning (2), varvid användarenheten (1) är an-
ordnad att registrera en signatur när användaren skriver
med användarenheten (1), och att skicka signaturen till
kontrollanordningen (2), som är anordnad att mottaga
10 signaturen, k ä n n e t e c k n a t av att kontroll-
anordningen (2) vidare är anordnad att bygga en signatur-
modell baserad på signaturen, att göra en kontroll av
signaturmodellens unikheter och att efter kontrollen avge
en signal, som indikerar signaturmodellens unikheter, till
15 användarenheten (1).

2. Systemet enligt krav 1, varvid signaturmodellen
är signaturen.

3. System enligt krav 1, varvid kontrollanordningen
(2) är anordnad att bygga upp signaturmodellen av ett
20 antal från samma användare mottagna signaturer.

4. System enligt något av föregående krav, varvid
kontrollanordningen (2) är anordnad att i kontrollen av
signaturmodellens unikheter beräkna minst en för signatur-
modellen kännetecknande parameter och att göra en kon-
25 troll av nämnda minst en parameter.

5. System enligt krav 4, i vilket kontrollanord-
ningen (2) är anordnad att i kontrollen av nämnda minst
en parameter kontrollera att nämnda minst en parameter
ligger över en förutbestämd unikhetsgränsnivå.

30 6. System enligt krav 5, varvid nämnda signal inne-
fattar information om vad användaren ska ändra på i sin
signatur för att nämnda minst en parameter ska hamna över
unikhetsgränsnivån.

7. System enligt något av föregående krav, varvid
35 kontrollanordningen (2) vidare är anordnad att klassifi-
cera signaturen.

2000 -03- 2 1

Huvudfoxen Kassar

17

8. System enligt något av föregående krav, varvid kontrollanordningen (2) är anordnad att, i kontrollen av signaturmodellens unikheter, jämföra denna med tidigare lagrade signaturmodeller.

5 9. System enligt något av föregående krav, varvid signaturen registreras som en sekvens av koordinater som beskriver användarenhetens (1) förflyttning när användaren skriver sin signatur med användarenheten (1).

10 10. System enligt något av föregående krav, vidare innefattande ett underlag (5), vilket är försett med ett positionskodningsmönster (7), som möjliggör beräkning av koordinaterna och från vilket användarenheten (1) är anordnad att registrera sekvensen av koordinater.

15 11. System enligt något av föregående krav, varvid användarenheten (1) innefattar en optisk sensor (14) och bildbehandlingsorgan (16) för registrering av signaturen.

12. System enligt något av föregående krav, varvid kontrollanordningen (2) är anordnad i en verifikationsdatabas.

20 13. Kontrollanordning för analys av en användares signatur, som är inskriven med en användarenhet (1), varvid kontrollanordningen (2) är anordnad att mottaga signaturen, k ä n n e t e c k n a d av att kontrollanordningen (2) vidare är anordnad att bygga en signaturmodell baserad på signaturen, att göra en kontroll av signaturmodellens unikheter och att avge en signal, som indikerar signaturmodellens unikheter, till användarenheten (1).

30 14. Kontrollanordningen enligt krav 13, varvid signaturmodellen är signaturen.

15. Kontrollanordningen enligt krav 13, varvid kontrollanordningen (2) är anordnad att bygga upp signaturmodellen av ett antal från samma användare mottagna signaturer.

35 16. Kontrollanordning enligt något av kraven 13-15, vilken är anordnad att i kontrollen av signaturmodellens unikheter beräkna minst en för signaturmodellen känneteck-

2000 -03- 2 1

Huvudfaxen Kassar

18

nande parameter och att göra en kontroll av nämnda minst en parameter.

17. Kontrollanordning enligt något av kraven 13-16, varvid nämnda signal innefattar information om vad användaren ska ändra i signaturen för att den ska uppnå en bestämd unikhets.

18. Kontrollanordning enligt något av kraven 13-17, vilken är anordnad i en verifikationsdatabas.

19. Sätt att analysera en signatur innefattande
- 10 stegen
- att med en användarenhet (1) registrera en signatur, att skicka vidare en representation av signaturen till en kontrollanordning (2), att i kontrollanordningen (2) bygga upp en signaturmodell,
- 15 att i kontrollanordningen (2) göra en kontroll av signaturmodellens unikhets och, att efter kontrollen avge en signal, som indikerar signaturmodellens unikhets, till användarenheten (1).
- 20 20. Sätt enligt krav 19, varvid kontrollen av signaturmodellens unikhets innefattar stegen att beräkna minst en för signaturmodellen kännetecknande parameter och, att göra en kontroll av nämnda minst en parameter.
- 25 21. Sätt enligt något av kraven 19 eller 20, innefattande steget att klassificera signaturen.
22. Sätt enligt något av kraven 19-21, innefattande steget att jämföra signaturmodellen med tidigare lagrade signaturmodeller.

2000 -03- 2 1

Huvudfaxen Kassan

19

SAMMANDRAG

Ett system för analys av en användares signatur.

- 5 Systemet innefattar en användarenhet (1) och en kontrollanordning (2). Användarenheten (1) är anordnad att registrera en signatur när användaren skriver med användarenheten (1) och att skicka signaturen till kontrollanordningen (2). Kontrollanordningen (2) är anordnad
- 10 att mottaga signaturen. Kontrollanordningen (2) är också anordnad att bygga en signaturmodell baserad på signaturen, att göra en kontroll av signaturmodellens unikheter och att efter kontrollen avge en signal till användarenheten (1). Signalen indikerar signaturmodellens unikheter.
- 15 het.

20

25

30 Publ.bild = Fig 1

Ink. t. Patent- och reg.verket

2000-03-21

Huvudfoxen Kassan

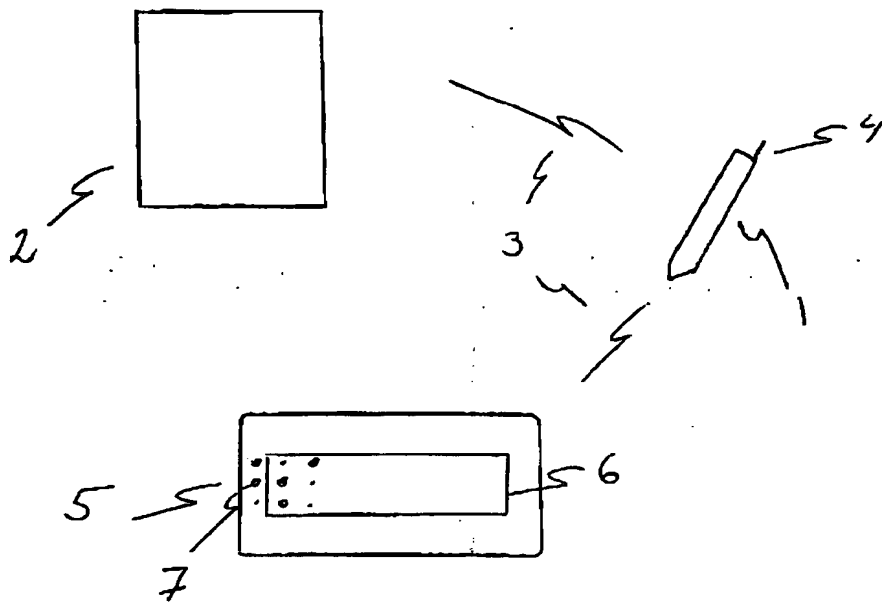


Fig 1

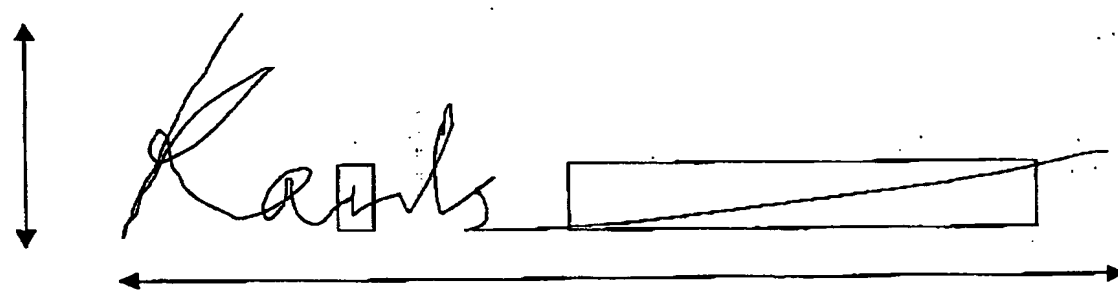


Fig 3

ink i Patent- och reg.verket

2000 -03- 2 1

Huvudfaxen Kassan

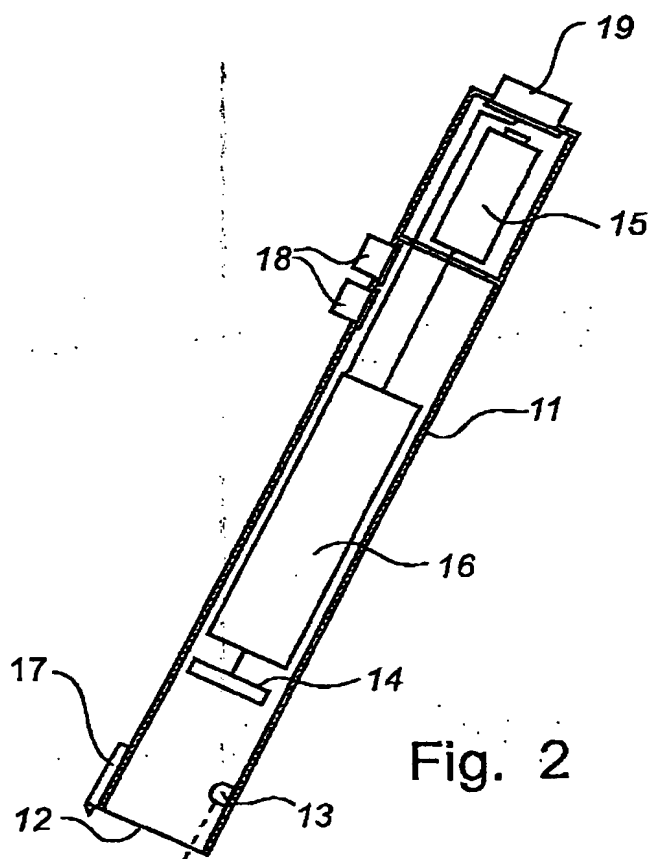


Fig. 2